



DEPARTMENT OF THE ARMY
HEADQUARTERS, EIGHTH ARMY
UNIT #15236
APO AP 96205-5236

REPLY TO
ATTENTION OF:

OCT 15 2013

EACG

MEMORANDUM FOR All Eighth Army and Subordinate Command Personnel

SUBJECT: Eighth Army Command Policy Letter #2, Operations Security (OPSEC) Policy

1. References:

a. Department of Defense (DOD) Directive 5205.02E, DOD Operations Security (OPSEC) Program, 20 June 2012.

b. DoD Manual 5205.02M, DOD Operations Security (OPSEC) Program Manual, 03 November 2008.

c. Joint Publication 3-13.3, Operations Security, 12 January 2012.

d. Army Regulation 530-1, Operations Security, 19 April 2007.

e. Combined Forces Command Operations Publication 3-4.9, Operations Security, 01 January 2007.

f. Army in Korea Regulation 530-1, Operations Security, 09 January 2012.

2. Purpose. The OPSEC program's primary purpose ensures the command practices OPSEC in order to deny critical information to adversaries.

3. Background. The OPSEC process is a proven means to protect operations and planning information and support Eighth Army's armistice and wartime missions. Individuals and staffs will analyze each operation and determine the appropriate level of risk. Commanders and Senior Leaders will actively participate in the program by providing guidance and decisions to ensure continuous protection of critical information and OPSEC indicators. OPSEC is:

a. Used to deny enemy intelligence information about friendly capabilities, intentions, and operations. Eighth Army accomplishes this by protecting indicators associated with planning and the conduct of military operations.

b. Integrated into the planning and execution phases of all military operations.

c. Include frequent evaluations and identification of Essential Elements of Friendly Information (EEFI). OPLANs are evaluated and refined annually in order to develop critical information specific to that plan.

d. Considered in the day-to-day operations of each organization.

EACG

SUBJECT: Eighth Army Command Policy Letter #2, Operations Security (OPSEC) Policy

4. Discussion.

a. Eighth Army members must understand that sensitive unclassified information requires protection and denial from adversaries. Small bits of information can be fused together to reveal a larger picture.


b. The successful enforcement of OPSEC procedures reduces the chance of serious injury and possible death of Eighth Army service members, damage to key infrastructures, or loss of critical technological capabilities.

5. Applicability. This policy applies to Eighth Army military members, DOD Civilian employees, contractors, Eighth Army dependents, and all those supporting Eighth Army operations.

6. Proponent. The proponent of the policy is the Eighth Army G33 at commercial 011-822-7913-3882 or DSN 315-723-3882.

Encls

- A. Eighth Army Critical Information List
- B. Eighth Army OPSEC Protective Measures



BERNARD S. CHAMPOUX
Lieutenant General, USA
Commanding

Enclosure A

Eighth Army Critical Information List (CIL)

1. General Officer and Civilian equivalent movements (Travel Itineraries and Schedules)
2. Exercise activities, scenarios, events, and results
3. Force compositions, status, movements, and locations
4. Logistics movements and locations
5. Presence or employment of new/ improved technology
6. Estimates in the effectiveness of operations
7. Telephone and radio communications, equipment, procedures, infrastructure and computer network IPs
8. Personal Information: Social Security Number, financial, legal, family, etc.

Enclosure B

Eighth Army OPSEC Protective Measures

The following OPSEC measures are integrated into our daily operations by all Eighth Army personnel. Vigilance in these six areas mitigates or reduces possible disclosures of sensitive information and operational indicators.

1. Computer Network Activities:

- a. Use the appropriate secure network (i.e. SIPRNET, CENTRIX-K) anytime you process classified information. This is the preferred method when working on or transmitting sensitive unclassified information.
- b. As a minimum, encrypt NIPRNET emails using your Command Access Card (CAC card) every time you pass sensitive information and unit Critical Information. This information will not be transmitted using commercial internet service providers.
- c. Properly label and control removable computer media (i.e. CD/DVD, removable hard drive, etc.) to protect sensitive unclassified and classified information.

2. Telephone and Radio Communications:

- a. Use a secure telephone (STE, VoIP, or vIPer) or encrypted radio for passing sensitive information.
- b. Do not attempt to "talk around" classified or sensitive information on an open line.
- c. Announce "phone up/ down" and use push-to-talk handsets properly.
- d. If cellular phones are authorized in the facility, power down (remove battery) and properly store the device in designated areas prior to entering classified working area or where classified or sensitive discussions take place.

3. Public Information Releases:

- a. Get approval from your chain of command before talking with any media representative. Refer all requests for information to the Public Affairs Office (PAO).
- b. Do not post sensitive operational information or information that could target friendly forces or family members to official publicly accessible or personal websites, weblogs, or chat rooms.
- c. Keep sensitive discussion in the workplace.
- d. Conduct periodic web content review in coordination with PAO IAW unit policies.

4. Document Disposal: Shredded papers are of no use to our adversaries. Shred 100% of all documents or paper that are work related or contain personal information (duty rosters, mailing addresses, social security information).

5. Know Critical Information: Know what to protect; post the command/unit Critical Information List (CIL) at all desks and workstations where information is processed and transmitted.
6. Immediately report all suspicious activities, persons, and objects to security manager and OPSEC officer.